

普通高等学校本科专业设置申请表

校长签字：

学校名称（盖章）：南宁学院

学校主管部门：广西壮族自治区

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-19

专业负责人：李建

联系电话：15877145559

教育部制

1. 学校基本情况

学校名称	南宁学院	学校代码	11549
主管部门	广西壮族自治区	学校网址	https://unn.edu.cn
学校所在市区	广西南宁龙亭路8号	邮政编码	530200
学校办学基本类型	☐ 教育部直属院校 ☐ 其他部委所属院校 ☒ 地方院校 ☐ 公办 ☒ 民办 ☐ 中外合作办学机构		
已有专业学科门类	☐ 哲学 ☒ 经济学 ☐ 法学 ☒ 教育学 ☐ 文学 ☐ 历史学 ☐ 理学 ☒ 工学 ☐ 农学 ☐ 医学 ☒ 管理学 ☒ 艺术学		
学校性质	☐ 综合 ☒ 理工 ☐ 农业 ☐ 林业 ☐ 医药 ☐ 师范 ☐ 语言 ☐ 财经 ☐ 政法 ☐ 体育 ☐ 艺术 ☐ 民族		
曾用名	邕江大学		
建校时间	1985	首次举办本科教育年份	2013年
通过教育部本科教学评估类型	合格评估	通过时间	2019年11月
专任教师总数	1023	专任教师中副教授及以上职称教师数	233
现有本科专业数	40	上一年度全校本科招生人数	5480
上一年度全校本科毕业生人数	2722		
学校简要历史沿革	学校建于1985年，原名邕江大学，2009年南宁市政府和民革广西区委共建，2012年升格本科。学校位于南宁市，是一所地方性、应用型本科高校，有区级一流专业建设点和重点特色专业13个，系广西新增立项建设硕士学位授予单位、广西新建本科学校转型发展试点学校、广西深化创新创业教育改革示范高校。		
学校近五年专业增设、停招、撤并情况	一、增设情况。2024年增设：智能车辆工程、智能建造；2023年增设：体育教育、大数据管理与应用；2022年增设电子信息工程、食品营养与健康、学前教育；2021年增设：新能源汽车工程；2020年增设：机器人工程、新媒体艺术、金融科技。 二、学校无停招、撤并情况。		

2. 申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	信息工程学院		
学校现有相近专业情况			
相近专业1专业名称	计算机科学与技术（注：可授理学或工学学士学位）	开设年份	2012年
相近专业2专业名称	物联网工程	开设年份	2014年
相近专业3专业名称	-	开设年份	-

3. 申报专业人才需求情况

申报专业主要就业领域	1. 政企安全防护：政府机构、大型企事业单位的网络安全部门，负责信息系统安全建设、运维、监控、应急响应与安全管理。 2. 互联网与科技公司：大型互联网企业、云计算服务商、科技公司的安全团队，聚焦产品安全、业务风控、数据安全、云安全、漏洞挖掘与修复。 3. 金融行业：银行、证券、保险等机构的网络安全部门，保障核心业务系统、支付安全、客户数据隐私及满足严格合规要求。 4. 安全企业：网络安全公司（如防火墙、入侵检测、态势感知、数据安全等产品厂商），从事安全产品研发、渗透测试、安全服务、安全咨询、威胁情报分析。 5. 测评与监管机构：信息安全测评中心、等级保护测评机构、通信管理等单位，进行安全风险评估、等级测评、合规审计与监管支撑。 6. 新兴领域：工业互联网安全、物联网安全、车联网安全、人工智能安全等方向的专业安全研究与防护。
人才需求情况	随着信息化和网络化的发展，网络空间安全已成为全球性政治博弈的新战场、军事对抗的新手段和经济竞争的新领域。目前，我国面临着网络空间安全

	相关专业人才历史存量过低、实战型网络空间安全人才严重不足等一系列问题。根据2022年发布的《网络安全人才能力白皮书》（2022版），到2027年，我国网络安全人员缺口将达327万，而高校人才培养规模每年仅3万人左右，高达92%的企业认为自己缺乏网络空间安全实战人才，因此，网络安全人才的培养已成为亟需解决的时代新命题。 作为一个新兴专业，网络空间安全专业人才供不应求，近三年网络空间安全相关专业本科生就业率为98%以上。根据2023年发布的《网络安全产业人才发展报告》（2023版），网络空间安全相关专业的毕业生规模约为1.45万人，远不能满足市场所需。毕业生可在政府机关、国家安全部门、银行、金融、证券、通信等领域从事复杂网络空间安全系统的设计、科学研究、技术开发、安全规划、运行维护、安全防御等方面的工作，也可以胜任保密理论研究、安全技术开发、安全组织管理、保密法规制定、等级保护等企事业单位信息安全相关岗位。 南宁学院作为南宁市市属唯一普通本科高校，2022年中共南宁市委网信办关于请予提供数字中国建设发展相关情况材料的函中，要求南宁学院提供网络空间安全人才培养的相关情况，以支撑南宁市数字中国的战略部署。目前学校已与多家企事业单位建立了用人合作关系，预测网络空间安全专业毕业生每年进入知名网络与信息安全公司工作，直接人才需求达115人。	
申报专业人才需求调研情况	年度招生人数	40
	预计升学人数	2
	预计就业人数	38
	广西宝信迪科技有限公司	12
	深圳融安网络科技有限公司	11
	华为	3
	广西泓源智能科技有限公司	12

4. 产业调研报告

一、引言

随着全球数字化进程的加速，网络安全已成为关乎国家主权、经济发展和社会稳定的核心议题，我国将网络安全上升为国家战略，是应对日益复杂的网络空间态势的必然选择。当前，企业数字化转型深入推进，组织与技术环境持续演变，特别是生成式 AI 技术的规模化应用，导致网络攻击暴露面与漏洞数量显著攀升，网络安全形势愈发严峻复杂。攻击规模不断扩大、手段日趋专业化，攻防对抗强度持续增加，我国重要行业和关键信息基础设施的安全面临前所未有的挑战。在此背景下，2025 年《网络数据安全条例》等政策法规的正式实施，进一步从制度层面强化了网络安全的战略地位，为行业规范发展与安全保障提供了法律依据。

本报告聚焦网络空间安全专业建设与产业发展的对接问题，旨在通过系统调研，为高校建设网络空间安全专业提供方向指引，促进人才培养与产业需求的精准匹配，从而有效缓解具备实战能力的网络安全人才不足这一制约产业发展的短板。调研范围将涵盖网络安全行业发展现状、关键技术演进趋势、产业人才需求特征以及高校专业教育改革路径等核心领域，以期为推动网络空间安全专业建设与产业发展的深度融合提供决策参考。

二、行业发展现状

（一）市场规模与增长趋势

中国网络空间安全市场规模呈现快速扩张态势，但不同机构基于统计口径与细分领域覆盖的差异，预测数据存在一定分化。艾媒咨询数据显示，2025 年市场规模预计达 786.4 亿元，2027 年将增至 884.4 亿元；另有报告指出 2025 年市场规模将突破 2500 亿元，2025-2030 年年复合增长率（CAGR）维持在 18% 左右；部分观点则认为受经济环境影响，2025 年市场规模将缓慢回升至接近 1000 亿元，增长率保持在 5% 以下。国际数据公司（IDC）预测，中国市场规模将从 2023 年约 840 亿元增长至 2028 年约 1400 亿元，CAGR 为 10.7%。全球市场方面，Gartner 预计 2025 年全球信息安全终端用户支出将达 1.5 万亿元，同比增长 15.1%。

市场增长主要受政策合规与数字化转型双轮驱动。政策层面，全球数据保护法规密集出台刺激合规需求，如 GDPR 相关服务市场 2025 年规模将突破 600 亿元；中国政策推动下，新兴经济体网络安全市场增速显著，2025-2030 年中国安全即服务（SECaaS）市场 CAGR 预计达 18.2%，高于全球平均水平。数字化转型方面，云安全、工业互联网安全等细分领域快速增长，云安全市场 2025-2030 年 CAGR 达 21.3%，从 420 亿元增至 1100 亿元；工业互联网安全市场规模有望从 2025 年 190 亿元跃升至 2030 年 550 亿元。

区域发展呈现显著不平衡特征。当前市场以长三角、珠三角、京津冀三大经济圈为核心，合计占比超过 60%，华东地区尤为集中，政府、金融、电信领域需求占比达 64%。新

兴市场潜力逐步释放，中西部地区增速高于全国平均水平，县域市场需求快速释放，杭州、成都等新一线城市网络安全设备采购增速超 25%，反映出区域市场从中心城市向次级区域扩散的趋势。

2025 年广西网络安全市场规模预计达 85 亿元，占全国市场的 1.08%，增速 12% 高于全国平均水平。其中，数据安全子市场规模 15 亿元，年增速 30%，金融、能源领域占比超 60%。自治区《工业领域数据安全能力提升实施方案（2024-2026 年）》要求 2026 年开展数据分类分级企业超 1000 家，重点行业网络安全人才需求年均增长 25%。南宁市作为中国—东盟信息港核心城市，数字经济企业达 1.93 万家，五象新区数字经济产值 640 亿元，算力中心度电补贴 0.15 元，吸引广西金普威（年营收 1.2 亿元）、广西实领安全（年需求渗透测试工程师 50 人）等企业集聚，形成覆盖安全集成、漏洞检测的产业生态。

（二）竞争格局与产业链

在竞争格局方面，本土企业在数据安全管控领域已形成显著技术优势。以明朝万达为代表的国内数据安全供应商，其数据安全产品在国内同类市场占有率连续多年保持较高水平，2021 年数据安全市场份额排名第二，数据泄露防护市场排名第三。头部企业如奇安信、启明星辰、深信服等凭借技术实力和品牌影响力占据市场主导地位，合计市场占有率超 30%，并在防火墙、威胁检测等细分领域形成差异化优势。同时，在政策支持下，本土企业加速技术突围，区域市场呈现梯度发展格局，华北、华东依托政务云与金融枢纽地位占据 70% 核心市场份额。

与国际领先企业相比，国内企业在高级威胁防护领域仍存在差距。国际头部企业如 Palo Alto Networks、Fortinet、Cloudflare 等通过平台化战略和技术整合不断扩大竞争优势，在全球市场占据领先地位，其中 Palo Alto Networks 于 2024 年以 559 亿元收购 CloudKnox 的案例进一步加速行业集中化。摩根士丹利对 Cloudflare、Fortinet、Palo Alto Networks 等国际领军者予以“增持”评级，反映其在高级威胁防护等关键领域的技术实力。

产业链结构呈现“上游依赖与中游创新并存”的特征。上游基础设施领域，半导体与基础软件仍由国际巨头主导，但国产替代进程加速，如中芯国际 14nm 工艺良率追平台积电，天科合达 SiC 衬底成本下降 30%。中游网络安全厂商向解决方案提供商转型，2023 年集成服务市场规模增长 22%，安全服务市场占比持续提升，预计 2030 年达到 42%，其中托管式安全服务（MSS）复合增长率高达 28%。下游应用领域高度集中，政府、金融、能源行业占需求总量的 65%，车联网、低空经济等新兴领域增速超 40%。

供应链安全对产业发展产生深远影响。使用非本地供应商的安全工具在应对复杂认证要求和地缘政治摩擦时面临更多挑战，这促使本土安全供应商巩固其在中国市场的主导地位。同时，全球网络安全行业集中度持续提升，2024 年二季度全球前十二大安全供应商市

场份额达 53.2%，较 2023 年同期上升 1.3 个百分点，中国网络安全行业集中度 CR5 预计从 2025 年的 38% 提升至 2030 年的 50%，头部企业通过并购整合技术能力成为行业趋势。

三、技术发展趋势

（一）AI 驱动的攻防变革

人工智能技术在网络空间安全领域呈现显著的“双刃剑”效应，攻防双方均加速引入 AI 技术，推动攻击手段智能化与防御能力自动化的深度变革。在攻击侧，生成式 AI（GenAI）的普及显著加剧了网络威胁的复杂性，不仅催生了大规模社会工程攻击、快速迭代的恶意工具等新型威胁，还通过高仿真攻击载体提升了攻击的隐蔽性。2024 年针对 AI 系统的攻击事件频发，如 Ray 框架漏洞被渗透控制 7000 余台服务器、Hugging Face Space 项目漏洞入侵、GPT 生成代码导致私钥泄露等，且 AI 应用漏洞攻击数量激增，Web 漏洞利用攻击拦截次数同比增长 68%，提示词注入攻击从泄露敏感信息升级为诱导系统权限调用的高危行为。据 Gartner 预测，到 2027 年，总体网络攻击中约 17% 将涉及生成式人工智能。

在防御侧，AI 技术通过机器学习算法自动检测异常行为、预测潜在威胁，利用自然语言处理分析安全日志，实时处理海量网络数据以识别恶意软件或钓鱼攻击，显著提升了防御效率与精准度。例如，Microsoft Security Copilot、Google SecOps、奇安信 AISOC 等 AI 安全产品通过数字员工实现 7*24 全天候监控告警，秒级研判分类，将安全告警响应时间从天级和小时级缩短至分钟级。天融信的 AI 驱动威胁检测准确率提升 70%，并能预测潜在攻击路径；英伟达 Morpheus 框架实时识别未加密数据泄露的效率比人工提升 10 倍。

AI 安全智能体与动态防御模型的落地成为应对智能化攻防的核心路径。安全智能体作为大模型在网络安全领域的重要应用，正朝着一体化解决方案方向发展，能够以虚拟安全专家形式拆解复杂安全需求，自主规划调度工具型智能体，独立解决 80% 的常规攻击事件。动态防御模型则推动防御从“规则维度”向“认知维度”升维，如网宿安全提出“AI+体系化主动安全”理念，构建“暴露面收敛—纵深防御—智能运营”动态防护架构，基于 WAAP、SASE 架构实现全流量威胁检测，并分区分域构建立体防护体系，已在潮玩商城、连锁企业等场景验证有效性。我国原创的内生安全理论和拟态构造技术也为构建自主可控的网络空间安全体系提供了新思路。从市场层面看，AI 驱动的威胁检测市场年增速有望达 30%，其安全产品市场份额预计从 2025 年的 15% 增至 2030 年的 40%，印证了技术落地的商业价值与行业需求。

实战应用中，CrowdStrike 引入“Charlotte”AI 安全分析师，通过赋能用户快速创建生成式 AI 工作流程，进一步验证了 AI 在提升安全运营效率中的实际价值。随着“以 AI 对抗 AI”成为行业共识，安全运营全流程 AI 化、数据标准统一化、AI 智能体工具化将成为未来发展重点，推动网络安全攻防进入智能化对抗新阶段。

（二）前沿技术突破

前沿技术突破正深刻重塑网络空间安全的技术格局，主要体现在量子计算对传统加密体系的冲击与应对、零信任架构对传统防御模式的革新，以及可信数据空间在数据跨境流动中的关键作用三个维度。

量子计算的快速发展对传统加密算法构成根本性威胁，其强大的并行计算能力可轻易破解基于大数分解和离散对数问题的 RSA、ECC 等主流加密算法。对此，全球已形成抗量子密码研发与应用的共识，美国国家标准与技术研究院（NIST）已选出首批抗量子加密算法，谷歌、IBM 等企业开始在浏览器和云服务中部署相关技术。中国在该领域亦有显著进展，2024 年抗量子密码相关专利数同比增长 50%，建成全球最大量子密钥分发（QKD）网络，并通过原创的内生安全理论和拟态构造技术形成差异化创新。企业层面，本源量子采用后量子密码学（PQC）混合加密方法，为第三代自主超导量子计算机“本源悟空”装备“抗量子攻击护盾”，量子加密技术已进入金融级应用验证阶段。

零信任架构（ZTA）作为对传统边界防御模式的革新，正逐步成为网络安全体系重构的核心。传统边界防御依赖“内网可信、外网不可信”的静态假设，难以适应云化、分布式网络环境下的威胁态势；而零信任架构基于“永不信任，始终验证”原则，通过持续身份认证、最小权限控制和动态访问授权，显著降低内部威胁与边界突破风险。市场数据显示，零信任架构的渗透率将从 2025 年的 30% 提升至 2030 年的 65%，相关解决方案市场规模预计突破 400 亿元，其与 SASE（安全访问服务边缘）等技术的融合应用，正成为企业数字化转型中的关键安全支撑。

可信数据空间作为数据跨主体共享与协作的重要载体，在数据跨境流动中发挥着基础性作用。其核心技术支持包括隐私计算、数据沙箱、高性能密态计算等，能够在保障数据主权与隐私安全的前提下，实现数据的可控流通与价值挖掘。企业实践中，蚂蚁集团等厂商已开始融合隐私计算、区块链与数据沙箱技术，构建安全可控的数据共享生态，为金融、医疗等敏感领域的跨境数据合作提供技术保障。尽管《可信数据空间发展行动计划》的具体内容未在摘要中详述，但可信数据空间的技术成熟度与应用范围持续扩展，正成为破解数据跨境流动合规性与安全性矛盾的重要路径。

（三）新兴场景安全

随着 5G 与物联网等新技术的深度融合，网络空间攻击面显著扩大，安全风险呈现多元化、复杂化特征。物联网设备的爆发式增长是攻击面扩大的核心诱因之一，2025 年全球物联网设备连接数量预计超过 250 亿个，涵盖智能家居（如智能门锁、摄像头）、工业传感器等多领域，此类设备因安全设计缺陷常成为攻击入口，例如智能门锁被破解、摄像头被用于窃取隐私等事件频发。同时，5G 网络漏洞可能引发大规模 DDoS 攻击和数据窃取，

API接口在设计与实现中的缺陷也易导致数据泄露，进一步加剧了攻击面的复杂性。

供应链安全风险成为新兴威胁焦点。硬件供应链中，恶意硬件植入可能造成物理杀伤性后果，需强化抗干扰通信协议建设；软件供应链则存在“多米诺效应”，高市场占有率产品的安全漏洞可能引发连锁反应，凸显更新流程测试与验证的重要性。攻击者还通过互联网暴露面结合 AI 生成的社工钓鱼攻击、供应链攻击等手段，突破 Web 应用防线形成全链路攻击闭环，对新兴场景安全构成严峻挑战。

在此背景下，行业定制化安全方案的市场潜力加速释放。工业控制系统安全是重点领域，2023 年美国宾夕法尼亚州阿利基帕市水务局因可编程逻辑控制器暴露遭黑客攻击，推动 2025 年相关防护体系建设加速，包括部署防火墙、入侵检测系统及完善漏洞管理、应急响应机制。边缘计算场景催生轻量化安全服务需求，预计将形成超过 358 亿元的新兴细分市场，物联网、车联网、工业控制等领域的安全需求呈井喷式增长。

融合领域安全引领市场增长，车联网、低空经济、卫星互联网等新兴领域安全需求增速超 40%。例如，车联网需针对性解决 OTA 升级漏洞、CAN 总线攻击等问题，低空经济则面临数据安全、隐私安全、系统安全等多重风险，需融合数据安全、通信安全技术及生成式 AI 提升智能化防御能力。可信数据空间通过隐私计算、数据沙箱等技术实现数据安全共享，推动新型商业模式涌现；零信任架构作为应对内部威胁的核心方案，2023 年市场规模达 42 亿元，金融、医疗行业渗透率超 60%，未来有望在各行业广泛应用。此外，供应链安全与跨境数据流动治理等细分市场潜力巨大，预计 2029 年规模可能突破 500 亿元。

四、人才需求与培养现状

（一）人才缺口与结构

我国网络安全人才供需矛盾显著，呈现数量缺口大、结构不匹配的特点。据 2022 年《网络安全人才实战能力白皮书》数据显示，目前国内每年的网络空间安全人才培养规模仅为 3 万人，许多行业面临着网络安全人才缺失的困境，到 2027 年，我国网络安全人员缺口将达 327 万。

企业对实战型人才的偏好突出，实战能力成为核心需求。从岗位分布看，实战型岗位主要集中在运维工程师、安全服务工程师、安全运营工程师等领域。招聘数据显示，83% 的安全运维岗位明确要求 3 年以上实战经验，而应届毕业生平均需 18 个月才能独立承担基础安全任务，反映出人才培养与企业实际需求的脱节。未来 3-5 年内，具备实战技能的安全运维人员与高水平网络安全专家将成为最稀缺和抢手的资源。

不同行业对网络安全人才的需求存在显著差异，关键基础设施和重点领域需求占比领先。能源行业的网络安全人才需求量占比最高，达 21%，其次是通信（16%）、政法（14%），金融行业占比 9%。此外，政务、网络企业、医疗卫生等行业需求占比分别为

7%、7%、6%，显示出能源、通信等关键行业在网络安全保障中的核心地位，以及金融等数据密集型行业对安全人才的稳定需求。

依托中国-东盟信息港，广西与东盟国家开展跨境数据安全合作，采用 SM2/SM4 国密算法保障中老铁路、中越边贸数据传输。2025 年广西公安机关计划招录网络安全职位 85 人，南宁高新区企业年需求网络安全工程师超 500 人，其中跨境数据安全分析师岗位薪资达 15000-25000 元/月，人才缺口占比 60%。

（二）薪资与就业质量

网络空间安全行业薪资水平整体较高且呈现显著差异化特征。猎聘数据显示，该领域人才平均薪资达 30 万+，高端岗位如安全架构师年薪可达百万。薪资水平受多重因素影响，具体表现为以下方面：

在经验维度，不同工作年限对应明显的薪资层级。初级职位（0-3 年经验）薪资范围约 8000-15000 元/月，涵盖网络安全运维、信息安全管理等岗位；中级职位（3-7 年经验）薪资提升至 15000-30000 元/月，如网络安全工程师、渗透测试工程师等；高级职位（7 年以上经验）薪资可达 30000-60000 元/月，一线城市顶级专家薪资更高，例如安全专家、首席信息安全官（CISO）等岗位。具体来看，新人月薪普遍为 6000-8000 元，1-3 年经验者可达 9700-10000 元，3-5 年经验者提升至 16700-26000 元，5 年以上经验者月薪普遍超过 30000 元。

认证资质对薪资的影响尤为突出。多数政企机构对注册信息系统安全师认证（CISSP、CISP）的重视程度远超学历、学位及毕业院校，持有 CISSP 证书的工程师薪资普遍高于行业平均水平 30% 以上，具备 CISP、CCSP 等认证的安全专家也拥有更高的薪资竞争力。

行业与地区差异同样显著。金融、政府、互联网、能源及通信行业薪资水平较高，如电信行业月薪可达 20000-50000 元。地区方面，一线城市薪资领跑全国，深圳网络安全工程师平均年薪 29.11 万元，北京、上海分别为 28.77 万元、28.16 万元，其中深圳 83.3% 的岗位月薪处于 15000-50000 元区间；二三线城市如成都、南京薪资涨幅明显，但整体水平较低，月薪多在 6000-15000 元。

职位类型与公司规模进一步加剧薪资分化。前沿领域岗位如 AI 安全架构师、量子安全工程师年薪轻松突破 80 万元，CISO 年薪 50 万起，部分顶尖人才可达百万；传统岗位中，渗透测试工程师月薪普遍 15000-30000 元，安全运维工程师月薪 10000-20000 元，数据安全工程师薪资比传统运维高 20%。公司规模方面，大型企业及互联网大厂薪资显著高于中小企业，大厂平均月薪 39000 元，最高月薪记录 47000 元，而地方政企单位如 2025 年江西省数盾信息技术网络安全研究院的解决方案工程师岗位薪资为 8000-18000 元/月。

人才流动方面，头部企业与中小企业的竞争态势明显。互联网大厂、金融机构等凭借

高薪（一线城市起薪普遍超过 1 万元/月）吸引大量人才，而中小企业及地方机构在薪资竞争力上相对弱势，面临人才争夺压力。整体来看，网络安全行业就业质量较高，44.7%的岗位薪资为 10000-30000 元/月，较全国平均工资高 65.1%，硕士岗位中 56.6%薪资达 20000-50000 元/月。

五、教育体系与改革方向

（一）专业建设现状

我国网络空间安全专业自 2015 年成为国家一级学科以来，呈现快速扩张态势，形成了涵盖信息安全、密码科学与技术、区块链工程等相关专业的体系，并通过一流网络安全学院建设示范项目（如西安电子科技大学、东南大学等首批 11 所院校及后续批次）推动学科发展。然而，专业规模扩张与教学资源不足的矛盾日益凸显。毕业生反馈显示，课程衔接需进一步优化，实践教学环节缺乏系统性实习实训项目，与企业合作资源有待拓展；普通本科院校普遍存在实践能力培养弱化问题，反映出实践平台、产业协同等教学资源的供给缺口。

在专业改革方面，部分院校已开展积极探索。西安邮电大学作为省级网络安全学院示范点，开设信息安全、网络空间安全等四个专业，建设无线网络安全技术国家工程实验室等平台，并展示真实网络业务场景下的安全技术实践环境，强化实战能力培养。成都信息工程大学推进本科教改，将“AI 赋能安全教材”、“产教融合课程”纳入建设方向，探索人工智能与网络安全交叉融合的课程体系。此外，西北工业大学立足学科优势提升实战型人才培养质量，武汉纺织大学与企业合作探索拔尖创新人才培养模式，为专业建设提供了多元化实践经验。

当前专业建设仍面临两项核心挑战：一是教材内容滞后于技术发展，行业技术快速迭代背景下，现有教材难以涵盖 AI 安全、网络空间治理等前沿领域，成都信息工程大学等院校已将“立体化教学资源建设”列为教改重点，反映出教材更新的迫切需求；二是师资实战经验不足，尽管部分院校拥有高水平教师队伍（如博士占比高、科研成果丰硕），但具备一线攻防、安全运维等实战经验的教师占比偏低，导致教学内容与产业实际需求存在脱节，这一问题在专业快速扩张背景下更为突出。

（二）教学改革实践

当前网络空间安全专业教学改革实践主要围绕 AI 赋能教学、实战化教学及跨学科融合三大路径展开，通过多元创新手段提升人才培养与行业需求的适配性。

在 AI 赋能教学方面，高校积极探索智能决策教材建设与课程体系重构。成都信息工程大学推进“AI 赋能安全视域下‘网络空间安全智能决策’教材建设”项目，将人工智能技术深度融入教学资源开发。西北工业大学以 AI 智慧课程为牵引，强化教学资源的数智化转

型，推动科教融汇与实战需求的结合。西安邮电大学则构建 AI 赋能的网络安全课程体系，通过智能技术优化教学内容与教学模式，提升教学精准度与学生学习效率。

实战化教学改革聚焦能力本位，构建多层次实践体系。校企合作层面，提出“需求导向、能力本位”优化路径，重点强化攻防对抗、威胁情报分析等核心技术模块的实战训练。平台建设方面，部分高校搭建网络攻防学赛训一体化创新平台，采用 OpenStack 等开源云架构，整合教学、实训、竞赛子系统，设计进阶通关式实践体系（初级涵盖信息安全法规与系统加固，中级涉及密码算法与系统安全，高级聚焦协议缺陷利用与漏洞分析），并配套 CTF 专题训练与能力导向实训（基础、综合、自主设计实训）。成都信息工程大学依托 CNNVD 漏洞案例库重构《网络安全攻防技术》课程，通过企业级攻防靶场开展实战演练，并推行“双导师制”（行业专家与教师共同指导），构建“漏洞预警—分析—复现—应急处置”全链条实践能力培养模式。职业本科教育进一步完善“课程实训-企业实习-项目实战”的能力递进通道，企业安全专家参与 60%实践课程教学，确保教学内容贴近业务应用。

跨学科融合方面，重点推进技术与法律、管理等领域的交叉培养。教育部《高等学校课程思政建设指导纲要》明确提出建设跨理学、工学、法学、管理学等门类的综合培养平台，强化非网络安全专业学生的安全知识技能教育。西安邮电大学将《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法律法规深度融入课程体系，培育学生“技术能力+法治素养”的双重素质。职业本科教育对接“等保 2.0”、数据安全法等最新标准，每学期更新 20%课程内容，确保技术教学与法律规范、行业标准紧密结合。

从人才培养质量提升效果看，上述改革路径有效弥补了传统教学模式中知识体系偏理论化、内容陈旧的不足。实战型培养方案基于行业专家经验，贴近业务应用，通过自主学习计划制定培养全栈型人才；校企合作与实践教学投入强化了学生的核心技术能力与问题解决能力；跨学科融合则拓宽了人才的知识视野与综合素养。例如，采用“需求导向、能力本位”的优化路径后，学生在攻防对抗、威胁情报分析等核心领域的应用能力显著提升；学赛训一体化平台的建设使学生在 CTF 竞赛等实战场景中表现突出，进阶式实训体系有效提升了学生从基础操作到漏洞分析的全流程能力。总体而言，教学改革实践通过多维度创新，显著提升了网络空间安全人才的培养质量，使其更适应行业对复合型、实战型人才的需求。

（三）政策支持与挑战

我国网络空间安全专业教育的发展离不开政策体系的系统性支撑，相关政策从法律法规构建、学科建设引导、产业需求对接等多维度为学科发展提供了保障。在法律法规层面，国家先后颁布《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等基础性法律文件，出台《网络安全审查办法》《云计算服务安全评估办法》

等配套政策，并制定 300 多项网络安全领域国家标准，形成了覆盖网络安全各环节的法律规范体系。其中，《网络安全法》首次以法律条款明确网络空间安全人才培养的重要性，为学科建设提供了法律依据。

在学科建设与人才培养专项政策方面，政策支持呈现出延续性与深化特征。2003 年《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）、2005 年教育部 7 号文件等早期政策奠定了信息安全人才培养的基础；2015 年《关于增设网络空间安全一级学科的通知》（学位【2015】11 号）将网络空间安全确立为独立一级学科，标志着学科建设进入规范化阶段。2016 年六部门联合印发《关于加强网络安全学科建设和人才培养的意见》，从加快学科建设、创新培养机制、强化师资队伍、推动校企合作等方面提出系统性举措，进一步明确了学科发展方向。此外，2017 年启动的“一流网络安全学院建设示范项目”、2023 年八部门《职业教育产教融合赋能提升行动实施方案（2023—2025 年）》提出的 19 条政策措施，以及 2021 年“职教 20 条”明确“2025 年职业本科招生规模不低于高职招生 10%”的目标，均从高等教育与职业教育协同角度强化了人才培养体系。在产业引导方面，2024 年修订的《产业结构调整指导目录》将“网络安全”新增为“鼓励类”行业，体现了政策对网络安全产业发展的直接推动，且 2024 年政策更注重行业细化落地与数据安全保护实效。

尽管政策体系不断完善，网络空间安全专业教育在落实过程中仍面临多重挑战。其一，校企协同机制尚未健全，企业参与人才培养的积极性不足，产学合作深度有限，导致教育供给与产业需求脱节。其二，实践教学体系滞后，职业院校普遍存在实践环境搭建困难（需部署专用虚拟机及工具，维护成本高）、实验项目陈旧（以验证性实验为主，与行业实战需求脱节）、综合实战能力培养不足等问题，且靶场资源分散，难以支撑系统化实践教学。其三，师资与教材建设存在短板，“双师型”师资（兼具理论教学能力与行业实践经验）数量不足，教材体系不完善，思政教育融入不足，且缺乏高水平人才培养基地支撑。其四，人才结构与质量有待优化，一方面存在人才数量缺口，另一方面能力结构不合理，如职业本科教育中理论基础的深度与广度不足，导致学生复杂问题分析能力较弱，课程体系对法律、管理、心理学等跨学科知识的整合不足。此外，宏观层面的安全责任分配机制、法律法规完善度、安全标准建设仍需提升，产业结构中高端产品与服务供应不足、中小企业实力较弱，以及资本投入匮乏、用户安全意识尚未完全成熟等问题，也对学科教育的落地成效形成制约。

六、政策环境与国际对比

（一）国内政策框架

国内网络空间安全政策体系已形成以《网络安全法》《数据安全法》《个人信息保护

法》为核心，辅以《关键信息基础设施安全保护条例》《网络数据安全条例》等法规的多层次框架，并建立关键信息基础设施安全保护、网络安全审查、网络安全服务认证等配套制度，制定发布 300 多项国家标准，为企业合规与市场发展提供明确指引。其中，2024 年 9 月公布的《网络数据安全条例》（2025 年 1 月 1 日施行）作为重要配套法规，进一步细化企业合规义务，包括明确重要数据的定义（特定领域、群体、区域或一定精度规模，可能危害国家安全等的的数据）及识别、申报、风险评估流程，优化数据跨境流动机制（建立国家数据出境安全管理专项工作机制），并规定网络平台服务提供者需设置个性化推荐关闭选项、发布社会责任报告等义务，同时明确国家网信部门统筹协调、公安、国安、数据管理部门按职责监管的分工体系，从操作层面强化企业数据安全主体责任落实。

政策体系的完善对网络安全市场需求形成显著拉动。一方面，《网络安全法》《数据安全法》等法律推动企业合规性投入显著增加，特别是关键信息基础设施行业（能源、金融、交通等）受“等保 2.0”和关基保护条例约束，网络安全投入占比预计从 2025 年的 35% 提升至 2030 年的 45%。另一方面，政策细化催生新兴需求，如《数据安全法》实施推动网络安全即服务（SECaaS）市场增长，而金融、能源等重点行业为满足数据分类分级、跨境流动规则等合规要求，进一步加大在安全技术研发、风险评估、应急响应等领域的投入，形成“政策合规-需求释放-市场增长”的正向循环。此外，地方与行业政策协同发力，如 2024 年江西省工业和信息化厅印发《江西省工业领域网络安全促进政策》，国家能源局印发《电力网络安全事件应急预案》，国家金融监督管理总局颁布《银行保险机构数据安全管理办法》，进一步聚焦细分领域安全需求，推动网络安全市场向专业化、纵深化发展。

（二）国际政策与竞争

当前全球网络空间安全领域的政策导向与国际竞争呈现显著差异化特征，主要国家围绕供应链安全、技术自主可控及规则主导权展开深度博弈。美国政策体系以强化供应链安全和网络弹性为核心，通过立法、资金投入与实战演练构建多层次防御体系。自 2013 年第 21 号总统政策指令首次明确“弹性”定义以来，美国持续发布《国家基础设施保护计划》《关键基础设施安全和弹性指南》等系列文件，将网络安全责任从使用侧向设计侧转移，同步推进设计安全与零信任架构。2024 年拜登政府发布的网络安全行政令进一步延续这一方向，要求提高第三方软件供应链透明度（如通过 CISA 的 RSAA 认证）、推动联邦系统采用零信任架构与后量子密码技术，并利用人工智能提升防御能力。在资源投入上，美国 2025 财年计划拨款 130 亿美元（约 932 亿元人民币）用于网络安全，同比增长超 10%，并通过“网络风暴”、“网络旗帜”等实战演练强化应对能力。此外，美国通过 2025 年 4 月生效的 EO14117 行政令及配套《最终规则》，将中国列为“受关注国家”，推动数据领域“局部

脱钩”，限制敏感数据流向中国，对在美中国企业构成直接合规风险。

中国则采取合规与发展平衡的政策路径，依托区域合作与“一带一路”倡议拓展市场空间，同时注重安全解决方案的国际化输出。在区域层面，中国通过 RCEP 框架推动东南亚市场关税降至 5%，并支持企业如大疆在曼谷落地“无人机+VR”体验中心，深化技术应用场景合作。在安全能力输出方面，国内企业借力“一带一路”项目，向沿线国家提供智慧城市安全解决方案，但在芯片级可信计算等底层技术领域仍存在代际差距，制约了核心竞争力。

国际规则体系的演变对中国企业出海构成复杂影响。一方面，欧盟《网络韧性法案》（2024 年 12 月生效）、澳大利亚与韩国发布的国家网络安全战略等，推动全球网络安全标准趋严，国际厂商依托成熟合规认证体系加速渗透关键基础设施领域，对中国企业形成竞争压力。另一方面，数据本地化要求与地缘政治驱动的“脱钩”政策（如美国 EO14117）显著增加了中国企业的跨境数据流动成本。世界经济论坛报告显示，54%的大型组织将供应链依赖视为网络弹性的最大障碍，而三分之一 CEO 将网络间谍与知识产权盗窃列为首要关切，反映出全球网络安全环境的复杂性已成为企业国际化的核心挑战。在此背景下，中国企业需在技术自主创新（如应对 AI 驱动的网络钓鱼与深度伪造威胁）与合规能力建设之间寻求平衡，以把握“一带一路”等倡议下的市场机遇。

七、挑战与机遇

（一）产业面临的挑战

网络空间安全产业面临的挑战主要源于两大核心根源：教育体系与产业需求脱节，以及研发投入不足。这两大问题相互交织，共同制约了产业的可持续发展。

教育体系与产业脱节是人才供给侧的核心矛盾。一方面，人才培养模式存在显著缺陷，表现为实践环境搭建困难、实验项目陈旧，且教学内容重防护技术传授而轻实战能力培养。职业本科教育虽为重要补充，但仍面临理论与实践平衡不足、行业对接松散及跨学科融合欠缺等问题，导致培养的人才难以直接满足产业对复合型、实战型能力的需求。另一方面，用户及从业人员的安全知识体系化程度不足，50.60%的用户依赖自学，仅 28.99%接受过少量培训，进一步加剧了人才素质与行业要求的差距。这种脱节直接导致全球网络安全人才缺口高达 340 万，中国 2025 年缺口预计达 140 万人，且资深专家稀缺、培养周期长，严重制约行业深度发展。

研发投入不足则从技术供给侧削弱了产业竞争力。资本层面，政企客户安全投入普遍谨慎，2024 年预算紧缩导致企业融资放缓，中小企业尤其面临资本匮乏困境。这直接导致关键核心技术受制于人、安全防护体系不完善，高端产品和服务供应不足，产业结构与发展质量亟待改善。技术挑战的加剧进一步凸显了研发投入的紧迫性：2024 年高危及以上开

源软件漏洞占比超 40%，全球新增 CVE 漏洞 40009 个，勒索软件攻击黑色产业链成型且制造业受害占比达 27%。同时，AI 武器化（如 2024 年窃取凭证类钓鱼攻击激增 703%）、量子计算对传统加密算法的颠覆性威胁，以及物联网设备安全设计不足等问题，均对现有研发体系提出更高要求。

为缓解上述挑战，需从两方面推进解决路径。在人才层面，应强化职业培训体系，针对教育实践短板设计定向培训项目，弥补实验环境与实战经验的不足，同时加强行业与教育机构的对接，提升跨学科融合能力，系统性提升从业人员及用户的专业知识水平。在研发层面，需加大政策补贴力度，通过财政支持鼓励企业增加研发投入，重点扶持中小企业技术创新，缓解资本匮乏压力，逐步实现关键核心技术自主可控，完善安全防护体系，从根本上提升产业竞争力。

（二）发展机遇

当前网络空间安全行业在政策红利与技术融合的双重驱动下，正迎来多维度的发展机遇，市场规模持续扩张且结构不断优化。政策层面，《网络数据安全条例》等法规的落地为行业提供了明确的合规框架，国家对学科建设、人才培养的系统性支持（如校企合作培育“即插即用”型工程技术人才）进一步夯实了产业发展基础，地方层面如广西实施的数字新质生产力培育行动也为区域协同创新创造了条件。

技术融合方面，“AI+网络安全”已成为核心创新主线，AI 驱动的“体系化主动安全”策略推动防御模式从被动响应向主动预判升级，超 60%企业采用 AI 增强安全解决方案，在安全运营、渗透测试、漏洞分析等领域实现效能提升（如奇安信集成 DeepSeek 大模型优化安全能力）。同时，量子安全（量子密钥分发、抗量子密码）、区块链（分布式身份认证）、5G 与物联网安全等技术融合领域加速突破，推动防护效率提升 50%，为行业注入新增长动能。

市场机遇呈现结构性增长特征。从规模看，2027 年中国网络安全市场规模预计达 884.4 亿元，2025-2030 年全球网络安全即服务（SECaaS）市场规模将突破 1.1 万亿元，亚太地区年增长率超 30%。细分领域中，云安全、数据安全、工业互联网安全成为核心引擎，其中云安全增速领先；新兴融合场景如低空经济、车联网、卫星互联网、算力网络等需求爆发，引领行业增长新方向。市场驱动逻辑已从合规主导转向需求及价值驱动，安全有效性验证、可信数据空间等新商业模式兴起，用户满意度持续提升（“比较满意”占比 54.72%， “非常满意”27.92%），进一步释放市场潜力。

国际拓展方面，中国网络安全企业凭借技术积累和成本优势，在东南亚、中东等市场取得突破，海外营收年均增速有望保持 25%，预计 2025 年海外收入占比提升至 15%，“一带一路”倡议为全球协同防护网络构建提供了合作契机。

综合来看，企业应聚焦 AI 安全、工业互联网安全、数据安全等高价值场景，把握技术融合与新兴市场机遇，同时依托政策支持深化产学研合作，提升全球竞争力。

八、结论与建议

（一）主要结论

网络空间安全产业呈现两大关键发展特征。一是行业已从传统的“合规驱动”向“价值驱动”转型，企业需通过技术工业化、场景定制化、服务闭环化及 ESG 价值重塑实现可持续发展，未来将形成“合规驱动与技术创新双轮共振”的格局。二是 AI 技术深度渗透行业全链条，不仅驱动攻防变革，成为威胁来源与技术革新的核心动力，还与零信任等技术共同推动行业变革，催生新兴场景安全需求。

在产业升级过程中，人才培养发挥着关键支撑作用。当前行业人才缺口显著，预计 2027 年缺口达 327 万，高校培养与产业需求衔接不足的问题突出。为此，职业本科教育成为重要方向，校企合作通过资源整合、课程共建及实践教学等模式深化，同时教育体系逐步完善，政策支持学科建设，以提升人才质量，满足产业发展需求。

（二）高校专业建设建议

为满足网络空间安全产业对高素质人才的需求，高校需从课程体系、师资队伍、校企合作三方面系统推进专业建设改革。

在课程体系优化方面，应强化实战导向与前沿融合。建议增加综合性、设计性实验项目，推广学赛训一体化平台以强化实战对抗训练，确保教学内容对接行业技术前沿。同时，需融入 AI 安全、量子安全、云安全、物联网安全等前沿领域课程，通过案例教学与项目驱动实现理论与实践深度融合，培养学生应对复杂安全挑战的能力。

师资队伍建设应聚焦“双师型”能力提升。高校需加大网络安全领域高层次人才精准引进力度，同时聘请企业资深技术专家担任兼职教师，推动教师赴企业实践交流，构建兼具学术底蕴与实战经验的教学团队。

深化校企联合培养是提升人才适配性的关键路径。建议推行“双导师制”，联合头部企业开发课程、共建实验室及实训基地，开展定向实习与联合培养项目。例如，可共建人工智能安全工程师认证中心等实践平台，将企业技术标准与岗位需求融入培养全流程，输送“即插即用”型复合型人才。

此外，还需加强顶层设计，明确人才培养目标与标准，通过跨学科课程（如网络安全法律与伦理、网络安全经济学）打破学科壁垒，并完善实验室、实训基地等教学资源投入，为人才培养提供系统性支撑。

5. 申请增设专业人才培养方案

一、专业简介

网络空间安全专业以“攻防技术+工程实践”为核心，以密码学、系统安全、网络攻防、数据隐私保护及人工智能安全等先进技术为支撑，依托校企共建的网络安全靶场、攻防实训平台与威胁情报中心，通过真实网络攻防演练、渗透测试项目及“安全应急响应”、“数据安全治理”等实践任务，重点培养面向数字化社会的全场景安全防御与攻防对抗能力，服务关键信息基础设施保护、金融安全、云计算及工业互联网安全等领域需求。就业前景：（1）网络安全企业岗位：渗透测试工程师、安全研发工程师、威胁情报分析师；（2）政企机构安全部门岗位：网络安全运维主管、数据安全合规顾问、安全架构师；（3）监管与司法机构岗位：网络安全等级保护测评师、电子取证工程师、安全合规审计师；（4）新兴技术领域岗位：云安全解决方案专家、工业互联网安全研究员、智能汽车安全工程师。

二、培养目标

本专业旨在培养拥护党的基本路线，德智体美劳全面发展，服务区域经济社会发展需要，掌握网络空间安全基本理论、网络安全管理知识、网络安全法律，熟悉安全领域前沿发展动态，具有较强工程实践和系统开发能力。在此基础上利用学科基础知识和实践能力解决多领域交叉网络安全问题，胜任网络空间安全类工程技术和管理工作。培养出具有独立从事网络与信息系统的的功能分析、开发、测试、维护等能力的高素质工程应用型人才。

学生毕业五年后，能够通过终身学习来顺应社会发展，能够适应独立和团队工作环境，能够顺利完成工程师的相关工作，同时应能够达到下列目标：

目标1—道德修养：具有良好的人文社会科学素养、社会责任感和工程职业道德，并在工程实践中遵守法律规范。

目标2—工程能力：能够综合运用专业及相关知识，解决网络空间安全相关领域的复杂工程技术问题，对网络空间安全领域的复杂工程项目提供解决方案。

目标3—工程与社会：能够评估网络安全工程活动对社会、健康、安全、法律文化和环境等因素的影响，以及工程方案的可持续性。

目标4—沟通与协作：能够融入和带领团队进行项目的实施，具有良好的沟通能力，能够在多学科团队和跨文化环境下工作。

目标5—自主学习：能够通过终身学习途径获取知识、提升能力、跟踪技术前沿和发展趋势。

三、毕业要求

本专业毕业生要求较好地掌握工科公共基础知识，较为系统地掌握网络空间安全基础

理论、基本技术和专业知识，接受从事网络空间安全技术应用相关的技能训练，初步具备综合运用基础理论和技术手段分析并解决实际工程问题的能力；掌握运用现代信息技术获取相关信息的能力；具有一定的管理能力和团队合作精神，并具有承担本领域的应用创新研究、软硬件产品的研发和生产的基本能力。

根据培养目标与培养定位，本专业的基本毕业要求如下：

1. 工程知识：具有从事网络空间安全技术工作所需的数学、自然科学、人文社会科学、工程基础和系统的网络空间安全专业知识，能够运用这些知识解决网络空间安全技术领域的实际工程问题。

2. 问题分析：能够应用网络空间安全专业的基本知识，理解网络空间安全的概念及模型，并能运用密码学和计算机网络的基本原理分析其合理性，提出实际的网络空间安全应用问题的解决方案，并获得有效结论。

3. 设计/开发解决方案：能综合运用所学理论知识，针对网络空间安全工程领域复杂工程问题的设计出满足应用需求和系统安全需求的解决方案。能够在设计环节中体现创新意识，并考虑社会、健康、安全、法律、文化以及环境等因素。

4. 科学研究：能够采用科学方法对网络空间安全工程领域工程问题进行科学研究，包括设计实验、分析与解释数据、并综合得到合理有效的结论。

5. 使用现代工具：能够针对网络空间安全工程领域工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和安全技术工具，利用安全工具对复杂工程问题进行建模、分析，并理解模型和方法的局限性。

6. 工程与可持续发展：能够基于网络空间安全工程相关背景知识进行合理分析，评价本专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律及文化的影响，并理解应承担的责任，了解国家在网络空间安全领域的法律法规，在从事职业过程中能遵守相关的法律法规要求。能够理解和评价针对网络空间安全工程领域复杂工程问题的专业工程实践对环境、社会可持续发展的影响。

7. 职业规范：具有人文社会科学素养和社会责任感，能够在网络空间安全工程实践中理解并遵守工程职业道德和规范，履行责任。

8. 个人和团队：具有团队合作精神或意识，能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。

9. 沟通：能够就网络空间安全技术领域中涉及的问题进行清晰表达，能够与业界同行及社会公众有效沟通和交流，具备结合本专业知识和撰写书面报告和口头陈述的能力，并具有一定的国际视野，能够在跨文化背景下进行沟通和交流。

10. 项目管理：理解并掌握网络空间安全工程管理与经济学知识，并能在多学科

环境中应用。

11. 终身学习：具有自主学习和终身学习的意识，有不断学习和适应发展的能力。

四、毕业要求对培养目标支撑矩阵

毕业要求对培养目标的支撑

培养目标 毕业要求	本专业培养目标				
	培养目标1	培养目标2	培养目标3	培养目标4	培养目标5
毕业要求1		√	√		√
毕业要求2		√	√		
毕业要求3		√			
毕业要求4			√		√
毕业要求5		√			
毕业要求6			√		
毕业要求7	√		√		
毕业要求8	√			√	
毕业要求9	√			√	
毕业要求10				√	
毕业要求11		√			√

五、毕业要求实现矩阵

毕业要求实现矩阵

毕业要求	能力实现支撑点(课程名称)
1. 工程知识：具有从事网络空间安全技术工作所需的数学、自然科学、人文社会科学、工程基础和系统的网络空间安全专业知识，能够运用这些知识解决网络空间安全技术领域的实际工程问题。	高等数学、大学物理、概率论及数理统计、线性代数、离散数学、电路电子技术、数字逻辑、计算机组成原理、程序设计与问题求解、数据结构、通信原理、网络空间安全数学基础
2. 问题分析：能够应用网络空间安全专业的基本知识，理解网络空间安全的概念及模型，并能运用密码学和计算机网络的基本原理分析其合理性，提出实际的网络空	信号处理、通信原理、数字逻辑、数据结构、数据库原理及安全、计算机网络、操作系统原理及安全、现代密码学、科技文献阅读与写作

间安全应用问题的解决方案，并获得有效结论。	
3. 设计/开发解决方案：能综合运用所学理论知识，针对网络空间安全工程领域复杂工程问题的设计出满足应用需求和系统安全需求的解决方案。能够在设计环节中体现创新意识，并考虑社会、健康、安全、法律、文化以及环境等因素。	程序设计与问题求解、面向对象程序设计、数据结构、微机原理与接口技术、计算机组成与系统结构、数据库原理及安全、操作系统原理及安全、网络空间安全导论、基础工程设计、专业工程设计
4. 科学研究：能够采用科学方法对网络空间安全工程领域工程问题进行科学研究，包括设计实验、分析与解释数据、并综合得到合理有效的结论。	电路电子技术基础实验、数字逻辑实验、大学物理实验、通信原理实验、计算机科学导论实验、程序设计与问题求解实验、微机原理与接口技术实验、数据结构、操作系统原理及安全、计算机网络、信息论与编码、网络安全、计算机科学导论
5. 使用现代工具：能够针对网络空间安全工程领域工程问题，开发、选择与使用恰当的技术、资源、现代工程工具和安全技术工具，利用安全工具对复杂工程问题进行建模、分析，并理解模型和方法的局限性。	电路电子技术、数字逻辑、通信原理、信号处理、程序设计与问题求解、面向对象程序设计、微机原理与接口技术、密码学及应用、网络安全
6. 工程与可持续发展：能够基于网络空间安全工程相关背景知识进行合理分析，评价本专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律及文化的影响，并理解应承担的责任，了解国家在网络空间安全领域的法律法规，在从事职业过程中能遵守相关的法律法规要求。能够理解和评价针对网络空间安全工程领域复杂工程问题的专业工程实践对环境、社会可持续发展的影响。	形势与政策、思想道德与法治、铸牢中华民族共同体意识、习近平新时代中国特色社会主义思想概论、马克思主义基本原理、毛泽东思想和中国特色社会主义理论体系概论、军事理论、网络空间安全导论、形势与政策、专业工程训练、生产实习、毕业设计
7. 职业规范：具有人文社会科学素养和社会责任感，能够在网络空间安全工程实践中理解并遵守工程职业道德和规范，履行	毛泽东思想和中国特色社会主义理论体系概论、中国近代史纲要、马克思主义基本原理、就业与创业指导、生产实习、专业

责任。	工程训练
8. 个人和团队：具有团队合作精神或意识，能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。	思想道德与法治、就业与创业指导、心理健康教育类课程、创新与创业类课程、职业生涯规划与规划
9. 沟通：能够就网络空间安全技术领域中涉及的问题进行清晰表达，能够与业界同行及社会公众有效沟通 and 交流，具备结合本专业知 识撰写书面报告和口头陈述的能力，并具有一定的国际视野，能够在跨文化背景下进行沟通和交流。	大学英语、美育与文化类课程、科技文献阅读与写作、计算机科学导论、专业工程设计、基础工程设计、相关双语教学与外文教材类课程、毕业设计
10. 项目管理：理解并掌握网络空间安全工程管理原理与经济学知识，并能在多学科环境中应用。	生产实习、经济与管理类课程、中国近代史纲要、专业工程设计、基础工程设计、毕业设计、计算机科学导论
11. 终身学习：具有自主学习和终身学习的意识，有不断学习和适应发展的能力。	职业生涯规划、计算机科学导论、就业与创业指导、毕业设计、现代密码学、网络空间安全导论、网络协议分析、人工智能导论

六、毕业条件及学位授予条件

（一）毕业条件

1. 思想品德考核合格；
2. 至少取得毕业学分为170学分；
3. 至少取得第二课堂学分20分，其中创新创业实践学分4学分；
4. 体质测试的综合成绩达标。

（二）学位授予条件

修业期满，经学校审核准予毕业，所有课程平均学分绩点达到2.0（含）以上，并且符合学校学位授予工作实施细则等相关规定。

七、主干学科

计算机科学与技术、密码学、信息与通信工程

八、核心课程

网络空间安全导论、离散数学、电路电子技术、数据结构、计算机网络、数字逻辑、

面向对象程序设计（Python）、网络空间安全数学基础、现代密码学、数据安全与隐私保护、网络攻击与防护、数据库系统原理及安全、密码学及应用

九、五育模块课程及第二课堂学分毕业要求

五育模块课程设置一览表

五育模块	性质	主要依托课程名称 (课程名称间用顿号隔开)
品德教育	必修	习近平新时代中国特色社会主义思想概论、中华民族共同体概论等思政类课程, 军事课(军事理论及军事技能)
	选修	(以讲座形式开展)
专业教育	必修	(具体见培养方案教学计划表)
	选修	(具体见培养方案教学计划表)
身心素质	必修	预防艾滋病健康教育课、大学生心理健康教育、大学体育 I-IV。
	选修	体育养生与运动健康系列、生命关怀与成长教育系列
人文审美教育	必修	(以讲座形式开展)
	选修	人文社科与艺术素养系列
通用能力(含劳育)	必修	劳动教育、国家安全教育、人工智能导论、创新创业基础、职业生涯发展和就业指导、沟通与写作(限定选修课)
	选修	自然科学与工程技术系列 英语数学能力高阶课程系列 创新创业与职业规划系列

通识选修课共8个学分, 包括体育养生与运动健康系列、生命关怀与成长教育系列、自然科学与工程技术系列、英语数学能力高阶课程系列、人文社科与艺术素养系列、创新创业与职业规划系列。

五育第二课堂学分毕业要求

第二课堂学分是学校全日制本科生必修的学分, 学生在校学习期间应至少获得第二课堂20个学分方可毕业。学生应根据自己的特长和爱好, 利用课外时间独立或在教师指导下参与品德素质、身心素质、人文审美素养、专业素质和通用能力等各类实践活动, 各模块的学分及活动形式(包括但不限于)见下表:

分类	第二课堂	学分	活动形式(包括但不限于)
品德素质	社会责任实践活动第1-6学期不少于1天/学期(每天0.5学分)	3	组织学生参与志愿服务、社会公益、道德讲堂等活动, 通过服务他人、回馈社

			会，培养学生的社会责任感、公民意识及高尚的道德情操。
身心素质	体育实践	4	包括体育竞赛、健身活动、心理健康教育讲座与团体辅导等，旨在增强学生体质，提高心理健康水平，培养积极向上的生活态度和坚韧不拔的意志力。
人文审美素养	人文艺术实践	3	组织文学艺术欣赏、书法绘画、摄影摄像、音乐舞蹈、戏剧表演等艺术实践活动，以及历史文化讲座、博物馆参观等，以丰富学生的文化底蕴，提升审美能力和人文素养。
专业素质 通用能力 (含劳育)	创新创业实践4学分 劳动实践活动（服务型劳动）第1-6学期不少于1天/学期（每天0.5学分）3学分 社会实践活动2学分 (大一、大二暑假各参加1周) 实验室安全培训。参加实验室安全知识学习培训并考核通过1学分。	10	1. 结合专业特色，开展专业技能竞赛、科研项目参与、学术论坛交流、企业实习实训等，帮助学生深化专业知识，拓宽专业视野，增强实践能力和创新能力； 2. 组织参加劳实践（服务型劳动）、社会实践、安全知训学习和培训； 3. 组织包括领导力培训、团队合作项目、公众演讲与口才训练、职业规划与就业指导等，旨在提升学生的领导力、团队协作能力、沟通表达能力及职业规划能力，为未来的职业生涯奠定坚实基础。
	合计	20	

十、课程设置及教学计划表

表1 网络空间安全专业教学进程计划表(必修部分)

课程类别	核心课程	课程名称	学分	总学时	学时分配		各学期学时分配								应修学分
					讲授	实践/实验	一	二	三	四	五	六	七	八	
通识必修课		思想道德与法治	2.5	40	40	0	40								42
		中国近现代史纲要	2.5	40	40	0		40							
		毛泽东思想与中国特色社会主义理论体系概论	3	48	48	0			48						
		习近平新时代中国特色社会主义思想概论	3	48	40	8					48				
		马克思主义基本原理	2.5	40	40	0				40					
		中华民族共同体概论	2	32	32	0	32								
		思想政治理论课实践教学	2	32	0	32			16	16					
		形势与政策1、2、3、4、5、6、	4	64	64	0	8	8	8	8	8	8	8	8	

	7、8															
	大学英语 1、2、3、4	12	192	192		48	48	48	48							
	体育 1、2、3、4	4	144	144		36	36	36	36							
	军事理论	2	36	36		36										
	职业生涯规划	1	16				16									
	就业与创业指导	1.5	24				24									
	通识必修课小计	42	748	668	40	200	172	148	148	56	8	8	8			
学科基础课	计算机科学导论	2	32	32		32										
	线性代数 B	2	32	32			32									
	★ 离散数学	4	64				64									
	高等数学 A1-A2	11	176	176		88	88									
	程序设计与问题求解	2	32	32		32										
	大学物理 B	4	64	64			64									
	概率论及数理统计	3	48	48				48								
	复变函数 B	2	32	32				32								
	★ 网络空间安全数学基础	2	32	32					32							
	人工智能导论	2	32	32			32									
	基础必修课小计	34	544	480	0	152	280	80	32							
专业必修课	★ 电路电子技术	3.5	56	56			56									
	★ 网络空间安全导论	3	48	48						48						
	★ 数字逻辑	3	48	48				48								
	★ 数据结构	3	48	40	8		48									
	★ 面向对象程序设计 (Python)	2.5	40	32	8			40								
	信号处理	3	48	48					48							
	★ 数据库系统原理及安全	3	48	40	8				48							
	微机原理与接口技术	3	48	48					48							
	操作系统原理及安全	3.5	56	48	8				48							
	★ 现代密码学	3	48	40	8					48						
	信息论与编码	3	48	40	8					48						
	通信原理	3	48	48					48							
	★ 计算机网络	3.5	56	48	8					56						
	网络安全	3	48	40	8						48					
	★ 数据安全与隐私保护	2	32	32	0					32						
	网络对抗原理	3	48	40	8						48					
	专业基础必修课小计	48	768	664	72	0	104	88	192	280	96	0	0			
必修课合计		124	2060	1844	112	376	524	316	380	336	104	8	8	8		124

注：表中有★的课程为核心课程。

表2 网络空间安全专业教学进程计划表（选修部分）

专业限选课	核心课程	课程名称	学分	总学时	学时分配		各学期学时分配								应修学分
					讲授	实践/实验	一	二	三	四	五	六	七	八	
		密码算法与分析（双语教学）	2	32	24	8						32			8
		机器学习	2	32	26	6					32				
		软件安全	2	32	26	6					32				
	★	密码学及应用	2	32	32						32				
		网络协议分析	2	32	32						32				
		无线网络攻防	2	32	16	16						32			
		科技文献阅读与写作	2	32	32							32			
		专业限选课小计	14	224	188	36	0	0	0	0	64	96	64	0	
专业任选课		网络空间安全前沿讲座	1	16	16						16			5	
		移动终端安全	2	32	16	16						32			
	★	网络攻击与防护	2	32	20	12						32			
		信息内容安全	2	32	26	6						32			
		操作系统安全	2	32	32						32				
		软件工程	2	32	32						32				
		密码分析	2	32	24	8							32		
		嵌入式系统及安全	2	32	32								32		
		信息隐藏与数字水印	2	32	32								32		
		网络编程技术	2	32	24	8							32		
	专业任选课小计	19	304	254	50	0	0	0	0	80	96	128	0		
通识选修课	全校通识选修课		通识选修课包括自然科学与技术工程类、人文与社会科学类、经济与管理类、心理健康教育类、创新与创业类、美育与文化六大类。 本专业要求在通识教育选修课程中选修8个学分，其中每个学生选修创新与创业≥2门，心理健康教育类≥1门，美育与艺术类≥2门，经济与管理类≥1 门。（若选修与本专业重复或相近的课程不计入学分）											8	

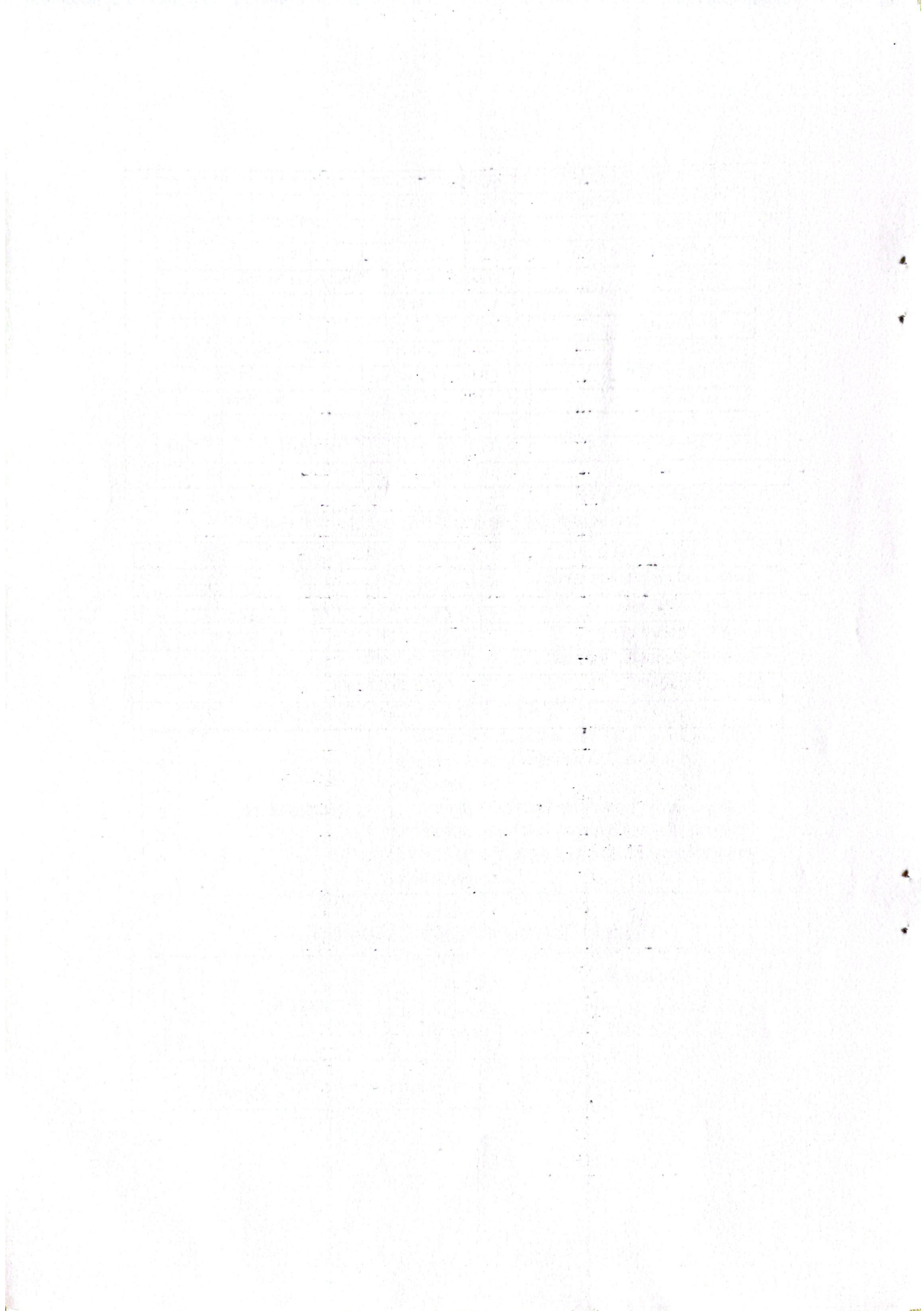
课程类别	核心课程	课程名称	学分	总学时	学时分配		各学期学时分配								应修学分	
					讲授	实践/实验	一	二	三	四	五	六	七	八		
		计算机科学导论实验	1	16		16	16									33
		大学物理实验	0.5	8				8								

实 践 环 节	程序设计与问题求解实验	1	16		16	16							
	电路电子技术基础实验	1	16		16		16						
	数字逻辑实验	1	16		16			16					
	微机原理与接口技术实验	1	16		16				16				
	信号处理实验	1	16		16				16				
	网络安全课程设计	2	32		32					32			
	密码算法课程设计	1.5	24		24						24		
	通信原理实验	1	16		16					16			
	基础工程设计	2	2周		2周					2周			
	生产实习	2	2周		2周						2周		
	专业工程设计	2	2周		2周							2周	
	毕业设计	16	16周		16周								16周
小计		33											

注：生产实习安排在第六学期暑假。

表4 网络空间安全专业培养计划总学时、学分数统计表

课程类别		学时数	学分数
通识课	通识必修课、通识选修课	748	42
基础课	学科基础课	544	34
专业必修课	专业基础必修课	768	48
专业选修课	专业限选课、专业任选课	208	13
实践环节	实践环节	33周（33×20=660）	33
合计		2928	170



6. 教师及课程基本情况表

6.1 专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
网络空间安全导论	48	4	李建	5
离散数学	64	4	韦铸娥	2
电路电子技术	56	4	呼大为	2
数据结构	48	4	陆涛	2
计算机网络	56	4	陈积常	5
数字逻辑	48	4	丛培勇	3
面向对象程序设计 (Python)	40	4	汪小威	3
网络空间安全数学基础	40	4	薛广明	4
现代密码学	48	4	李建	5
数据安全与隐私保护	32	4	邓鹏鹰	5
网络攻击与防护	32	4	沈艺敏	5
数据库系统原理及安全	48	4	李陶深	5
密码学及应用	32	4	李庆年	6

6.2 本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历 毕业学校	最后学历 毕业专业	最后学历 毕业学位	研究领域	专职/兼职
李建	男	1962-09	网络空间安全导论、现代密码学	教授	研究生	解放军信息工程大学	密码学	博士	密码学	专职
李陶深	男	1957-09	数据库系统原理及安全	教授	研究生	中南大学	计算机技术	博士	计算机技术	专职
薛广明	男	1985-06	网络空间安全数学基础	教授	研究生	陕西师范大学	运筹学与控制论	博士	应用数学	专职
汪小威	男	1985-01	面向对象程序设计	教授	研究生	泰国拉卡邦先皇技	技术增强学习与创	博士	计算机技术	专职

			(Python)			术学院	新			
陆涛	男	1982-10	数据结构	教授	研究生	泰国拉卡 邦先皇技 术学院	技术增强 学习与创新	博士	计算机技术	专职
陈积常	男	1982-09	计算机网 络	教授	研究生	广西大学	计算机科 学与技术	硕士	计算机网 络	专职
沈艺敏	男	1985-01	网络攻击 与防护	教授	研究生	广西大学	计算机科 学与技术	学士	网络安全	专职
李庆年	男	1975-05	密码学及 应用	教授	研究生	泰国格乐 大学	教育管理	硕士	计算机技 术	专职
邓舒婷	女	1985-07	操作系统 原理及安全	副教授	研究生	广西师范 大学	教育技术 学	硕士	计算机技 术	专职
魏小迪	女	1986-10	移动终端 安全	副教授	研究生	湖南师范 大学	教学技术 学	硕士	计算机技 术	专职
韦铸娥	女	1984-09	信息论与 编码	副教授	研究生	广西师范 大学	概率论与 数理统计	硕士	信息与编 码	专职
李杰	男	1979-07	网络协议 分析	副教授	研究生	清华大学	计算机科 学与技术	博士	网络安全	专职
郭磊涛	男	1983-10	机器学习	其他副高 级	研究生	中国科学 技术大学	计算机系 统结构	博士	机器学习	专职
丛培勇	男	1979-07	网络对抗 原理	其他中级	研究生	北京工业 大学	信息系统 安全	博士	嵌入式系 统安全	专职
邓鹏鹰	女	1991-06	信号处理 、数据安全 与隐私保 护	讲师	研究生	华中科技 大学	电子与通 信工程	硕士	信号处理	专职
呼大为	男	1981-08	电路电子 技术	未评级	研究生	中国科学 技术大学	计算机应 用	博士	电路与系 统	专职
孙寒冰	男	1985-02	嵌入式系 统及安全	未评级	研究生	装甲兵工 程学院	武器系统 与运用工 程	博士	嵌入式系 统安全	专职
张聪	女	1980-08	通信原理	未评级	研究生	国防科学 技术大学	信息与通 信工程	博士	电路与系 统	专职
李飞	男	1990-09	微机原理 与接口技	未评级	研究生	北京理工 大学	计算机科 学与技术	博士	信息安全	专职

			术							
李永久	男	1986-07	无线网络 攻防	未评级	研究生	西安电子 科技大学	电磁场与 微波技术	博士	信息安全	专职

6.3 教师及开课情况汇总表

专任教师总数	20		
具有教授（含其他正高级）职称教师数	8	比例	40.00%
具有副教授及以上（含其他副高级）职称教师数	13	比例	65.00%
具有硕士及以上学位教师数	19	比例	95.00%
具有博士学位教师数	13	比例	65.00%
35岁及以下青年教师数	2	比例	10.00%
36-55岁教师数	16	比例	80.00%
兼职/专职教师比例	0:20		
专业核心课程门数	13		
专业核心课程任课教师数	12		

7. 专业主要带头人简介

姓名	李建	性别	男	专业技术职务	教授	行政职务	无
拟承担课程	密码技术与应用			现在所在单位	南宁学院		
最后学历毕业时间、学校、专业	2008年12月毕业于中国人民解放军信息工程大学密码学专业，获得博士学位。						
主要研究方向	应用密码学、信息安全等级保护						
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	在负责密码装备保障人员的技术培训工作期间，将培训工作中积累的教学改革经验总结为“上好XX密码机技术保障课初探”等数十篇论文发表在军队《维修技术》和《机要装备管理》等学术刊物上，并将研究成果用于指导部队密码工程技术人员技术培训工作，被广州军区授予“军事训练标兵”荣誉。主持或参与“基于等级保护的信息安全课程体系探索与实践”等自治区级教学改革项目5项。发表“Cultivating Personal Capabilities Based on Problem-Based Learning: A Practice in Web Development”等教学改革论文。参与指导的南宁学院《智能交通预警及道路通行诱导系统》项目在首届中国“互联网+”大学生创新创业大赛广西选拔赛决赛中荣获金奖。						
从事科学研究及获奖情况	先后主持或参与“基于自主密码的可信计算平台的兼容性研究”、“网络信任体系建设相关策略研究”、“密码终端系统功能扩充”等国家863高技术研究发展计划项目和各级科研项目（18项）的研究工作；获得军队级科技进步三等奖3项，其中“传真机故障诊断专家系统”等2项成果填补了军队技术空白，并在军队推广应用。在国内外学术刊物上发表研究论文60余篇，其中数十篇论文被EI和ISTP检索及核心期刊上发表，参与撰写军队密码工程技术著作1部，研究论文获得南宁市科技论文三等奖。由于在科学研究上的突出成绩，先后被中国人民解放军总参谋部、总政治部授予“全军优秀硕士研究生”、“全军优秀机要干部”、“全军机要两个系统建设先进个人”等荣誉。荣立二等功一次，三等功五次。						
近三年获得教学研究经费（万元）	2.0			近三年获得科学研究经费（万元）	20.0		
近三年给本科生授课课程及学时数	《密码技术与应用》192课时、《网络安全》96课时、《通信系统安全实践》48课时。			近三年指导本科毕业设计（人次）	24		

姓名	李陶深	性别	男	专业技术职务	教授	行政职务	副校长
拟承担课程	数据库系统原理及安全			现在所在单位	南宁学院		
最后学历毕业时间、学校、专业	2008年6月毕业于中南大学计算机应用技术专业，获得博士学位。						
主要研究方向	数据库系统原理及安全						
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	广西高等教育自治区级教学成果奖9项（特等奖1项、一等奖2项、二等奖2项、三等奖4项）；第27届中国西部地区优秀科技图书二等奖1项，广西高校优秀教材奖2项（一等奖1项、二等奖1项），广西区级教改项目15项，主编出版专著1部、教材5部。						
从事科学研究及获奖情况	长期从事计算机科学与技术学科的教育与科研工作，目前研究方向为：云计算与大数据、无线网络理论与应用、分布式工程数据库、网络计算与信息安全等。先后发表学术论文700多篇，其中被SCI、EI检索收录200余篇。获国家发明专利6项，软件著作权登记成果10项。主持或主要参与国家级科研项目13项，省部级科研项目30多项。先后获广西科技进步奖3项（二等奖1项、三等奖2项），广西自然科学奖三等奖1项，铁道部铁路工程勘察设计计算机优秀软件三等奖1项，广西计算机应用推广奖三等奖4项。						
近三年获得教学研究经费（万元）	15.0			近三年获得科学研究经费（万元）	80.0		
近三年给本科生授课课程及学时数	《数据库原理》192课时			近三年指导本科毕业设计（人次）	24		

姓名	薛广明	性别	男	专业技术职务	教授	行政职务	副院长
拟承担课程	网络空间安全数学基础			现在所在单位	南宁学院		
最后学历毕业时间、学校、专业	2024年6月毕业于陕西师范大学运筹学与控制论专业，获得博士学位。						
主要研究方向	智能信息处理与模糊控制						
从事教育教学改革研究及获奖情况（含教改项目	薛广明，粟光旺，林福宁，“双一流”背景下财经类院校数学专业与课程协同建设的研究—以广西财经学院为例，前卫，2022，15，120-122.						

、研究论文、慕课、教材等)							
从事科学研究及获奖情况		2024.01-2027.12, 国家自然科学基金地区项目, 12361092, 分数阶模糊非线性系统预定义时间事件触发学习控制, 在研。 2023.06-2027.05, 广西自然科学基金面上项目, 2023GXNSFAA026174, 分数阶非线性系统的预定义时间模糊复合学习控制, 在研。 2022.01-2023.12, 广西高校中青年教师基础能力提升项目, 2022KY0651, 基于扰动观测器的分数阶不确定非线性系统复合学习控制, 已结题。					
近三年获得教学研究经费(万元)	5.0			近三年获得科学研究经费(万元)	56.0		
近三年给本科生授课课程及学时数	《高等数学》192课时、《离散数学》196课时			近三年指导本科毕业设计(人次)	15		
姓名	陈积常	性别	男	专业技术职务	教授	行政职务	副院长
拟承担课程	计算机网络			现在所在单位	南宁学院		
最后学历毕业时间、学校、专业	2005年7月毕业于广西大学计算机科学与技术专业, 本科、学士; 2016年6月桂林电子科技大学获得工程硕士学位。						
主要研究方向	计算机安全						
从事教育教学改革研究及获奖情况(含教改项目、研究论文、慕课、教材等)	积极探索应用型课程改革研究, 主持教育部产学研合作协同育人项目、全国高等学校计算机教育研究会项目、广西教育科学“十三五”规划项目5项, 课改成果丰硕。 1. 2021年广西高等教育自治区级教学成果一等奖(排名第二); 2. 2023年广西高等教育自治区级教学成果二等奖(排名第一); 3. 2022年自治区首批虚拟教研室(负责人); 4. 2023年自治区级课程思政示范基层教学组织(负责人); 5. 2019年广西线上线下混合一流本科课程《现代交换技术》(课程负责人); 6. 2022年广西线上一流本科课程《TCP/IP网络》(课程负责人); 7. 2022自治区课程思政示范课《现代交换技术》(课程负责人); 8. 2023年全国慕课十年典型案例奖(课程负责人); 9. 2023年广西数字技术与教育教学融合优秀案例(课程负责人);						

		10. 2024年度广西教育数字化转型优秀案例（负责人）； 11. 教育部第十届应用型课程建设大课堂说课展示活动一等奖（排名第一）； 12. 广西壮族自治区第二届高校教师教学创新大赛正高组二等奖（排名第一）。					
从事科学研究及获奖情况		主持广西高校中青年教师科研基础能力提升项目两项（2014年、2017年），2021年主持广西盛源行电子信息股份有限公司横向课题1项，总经费30万。发表《基于领域嵌入的循环膨胀卷积神经网络评价对象抽取方法》、《局部观测的车辆边缘计算在线服务迁移决策》等EI、中文核心等论文8篇，专著1部，软件著作权2项。					
近三年获得教学研究经费（万元）	30.0			近三年获得科学研究经费（万元）	30.0		
近三年给本科生授课课程及学时数	《TCP/IP网络》432课时、《现代交换技术》576课时。			近三年指导本科毕业设计（人次）	24		
姓名	陆涛	性别	男	专业技术职务	教授	行政职务	无
拟承担课程	数据结构			现在所在单位	南宁学院		
最后学历毕业时间、学校、专业	2025年3月毕业于泰国拉卡邦先皇技术学院技术增强学习与创新专业，获得博士学位。						
主要研究方向	软件工程、大数据技术						
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	主持于2016年度高等教育教学改革工程项目“基于校企协同育人的“混编型”师资队伍建设的研究与实践——以南宁学院中兴通信工程学院为例”，主持2020年度高等教育教学改革工程立项项目《基于“线上线下”模式的项目教学法在工程实践课程教学的研究与实践》，主持2021年第二批教育部产教融合协同育人项目《面向人工智能领域的校企“混编型”师资队伍建设》，主持校级教学团队建设项目《项目教学法实践教学团队》，发表《项目式教学法在数据科学与大数据技术专业课程教学的应用研究与实践》等教改论文8篇，作为主要参与《“双主体、共利弧、深融合”产业学院建设的探索实践》获自治区高等教育教学成果奖一等奖（排名第四），主持申报《基于智慧教育平台（博思智慧平台+AILab平台）的实践教学综合改革研究》获2021年南宁学院高等教育教学成果奖一等奖，获南宁学院高等教育教学成果						

		奖一等奖（排名第一）。	
从事科学研究及获奖情况		主持并于2023年结题2020年度广西高校中青年教师科研基础能力提升项目“基于大数据可视化技术的农产品物流减损监测与控制系统”，主持并于2019年结题2015年度广西高校科学技术研究项目“基于新媒体技术的多渠道农业生产资讯推送平台”，主持2020年南宁学院教授工程《基于统计特征分类耦合自适应Gamma校正的图像增强算法》，主持校级横向课题《基于图像增强技术的动画渲染处理系统》，主持校级横向课题《在线慕课系统研究开发》，主持校级横向课题《地区交通大数据分析统计系统》，主持校级横向课题《社区垃圾分类微信小程序系统》，发表《Protein function module of deep learning and PPI network prediction》、《基于统计特征分类耦合自适应Gamma校正的图像增强算法》等SCI、EI、中文核心等论文12篇，专著1部，软件著作权1项。	
近三年获得教学研究经费（万元）	11.4	近三年获得科学研究经费（万元）	32.0
近三年给本科生授课课程及学时数	《数据结构》192课时、《面向对象程序设计》192课时、《数据结构综合实践》72课时。	近三年指导本科毕业设计（人次）	24

8. 教学条件情况表

可用于该专业的教学实验设备总价值（万元）	543.87	可用于该专业的教学实验设备数量（千元以上）	533（台/件）
开办经费及来源	600万元，学校自筹经费		
生均年教学日常运行支出（元）	1800.0		
实践教学基地（个）	12		
教学条件建设规划及保障措施	学院根据《普通高等学校本科专业类教学质量国家标准》要求不断提高教学条件，加强基础设施建设。 1. 师资队伍建设：目前网络空间安全专业校内储备教师20人，其中教授8人，副教授或者其他副高级5人，学院与华为公司开展深度校企合作，已经形成校企结合稳定合理的学科梯队。同时组织专业教师参加大量相关专业培训、进修及国内外交流，结合内培外引，构建一支高水平的网络空间安全教学团队。 2. 课程体系建设：学校已经开设了部分网络空间安全主干课程，具备了比较丰富的教学资源。围绕网络空间安全人才培养目标定位，针对网络空间安全的专业核心课程教学需求，优先建设专业特色课程，积极培育精品课程，努力打造网络空间安全专业的“一流课程”。目前相关专业已获得《TCP/IP网络》《数据原理》《电工电子技术》等自治区一流本科课程5门。 3. 实践教学基地建设：目前学院拥有教育部ICT产教融合创新基地1个、广西协同育人平台1个，形成计算机技术、网络安全等多个专业实验室和研究中心。根据专业教学实验室的建设计划，有重点地逐步建立为专业教学所必须的设备齐全、管理规范的专业实验室，达到课程教学计划规定的要求，确保实验课的教学质量。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
Windows2008R2操作系统	*	2	2016	7.0
柜式空调	KFR-72LW/BDN8Y-PA401(2)A	2	2023	13.0
音响	ME44	1	2023	1.25
网络安全靶场平台	锐捷	1	2024	610.0
网络靶场服务器	锐捷	3	2024	240.0

网络安全人才培养课程 服务	锐捷	1	2024	50.0
防火墙	锐捷	1	2024	45.0
入侵防御设备	锐捷	1	2024	50.0
堡垒机	锐捷	1	2024	40.0
WEB应用防护墙	锐捷	1	2024	50.0
安全审计	锐捷	1	2024	50.0
上网行为管理	锐捷	1	2024	30.0
安全管理中心	锐捷	1	2024	80.0
千兆交换机	锐捷	1	2024	5.0
服务器密码机	锐捷	1	2024	150.0
签名验签服务器	锐捷	1	2024	80.0
VPN加密网关	锐捷	1	2024	200.0
密码学实验室配套	锐捷	1	2024	100.0
密码学实验课程	锐捷	1	2024	70.0
系统集成	锐捷	1	2024	10.0
微型电子计算机	启天M450-A225	25	2023	145.5
网络同传软件	OSS-V8	1	2023	57.6
电脑桌	*	13	2022	6.5
蓝牙无线接收机	HC-BTTX-600+RX	1	2021	1.15
激光投影机	XJ-VC330XS	1	2019	8.8
密码学辅助教学系统	*	1	2016	48.85
攻防实验客户终端	*	40	2016	74.0
攻防演示系统	*	1	2016	20.0
攻防实验管理系统	*	1	2016	38.3
攻防实验平台	DCST-6000-N60	5	2016	186.0
微型电子计算机	M4500-D620	41	2016	211.15
机柜	Ja6618 (Ja2000)	2	2011	2.27
机柜	Ja6942 (Ja2000)	1	2011	2.48
交换机	2918-24TT-C	1	2011	3.42
交换机	3750V2-24TS-S	1	2011	11.0
云终端软件	VDI接入	1	2023	21.0
宽屏投影幕布	ELMW1331609	1	2023	1.2
教师多媒体讲台	定制	1	2023	3.0

交换机	RG-S2910V2-48GT4SFP-L	1	2023	4.3
交换机	RS3300-52T-4F	1	2023	4.5
功放机	FS-150G	1	2023	1.25
投影机	P60	1	2023	27.5
云终端	aDesk-STD-200H-s (HDMI)	21	2023	76.65
云桌面管理服务器	VDS-R-7550	1	2023	92.0
教师讲台	定制	1	2023	3.33
电子教室管理软件	RG-CMR-Lic70	1	2023	8.98
云终端软件	RG-CDC-IDV-Lic	1	2023	29.07
云桌面管理平台软件 (U盘)	RG-CCP-DCP-Lic-EDU	1	2023	7.12
网络机柜	22U	1	2023	1.3
交换机	RG-S2910V2-24GT4SFP-L	2	2023	6.65
音箱	TK-1143	1	2023	1.9
功放	TK-1108K	1	2023	1.9
激光投影机	PT-BHZ611C	1	2023	28.5
学生云终端	RG-CT5500-G3	51	2023	363.38
云桌面管理服务器	RG-CS1020	1	2023	28.9
扩声音频处理器	DSP-AP3100R	1	2022	10.8
交换机	RG-S2900-24GT4SFP	2	2022	5.0
投影机	AL-LW320	1	2022	20.3
中央控制器	HC-E6000 (HD)	1	2022	3.6
微型电子计算机	启天M437-A440	51	2022	275.4
微型电子计算机	启天M433-A440	58	2022	324.8
交换机	RG-NBS3100-24GT4SFP	6	2022	13.8
信号系统与信号处理实验系统	RC-SS&SP-III	30	2021	288.0
通信原理教学实验系统	RC-TX-VI	30	2021	204.0
音箱	D-MAKE SP590	2	2021	3.9
中控系统	HC-E6000	1	2021	4.0

中控台	S600	1	2021	3.5
功率放大器	DSP-AP3100R	1	2021	7.5
投影机	AL-LW340	1	2021	23.64
微型电子计算机	M730e-A014	50	2021	300.0
云服务器	ThinkSystem SR550	1	2018	100.0
云终端	aDesk-STD-100	15	2018	60.0
无线话筒	Echor UPL-600+	1	2018	2.5
单人电脑桌	轩鑫706075	1	2018	0.3
中控	HS3000	1	2016	1.0
中控桌	TC-JTG11	1	2016	2.5
柜式空调	KFR-72LW/72520Aa-2	3	2016	19.5
音响	K-218A	1	2016	1.5
功率放大器	BK-2300	1	2016	1.5
电子白板	SBM685V	1	2016	18.5
宽屏短焦投影机	CB-585W	1	2016	13.5
管理软件	*	1	2016	35.0
云终端一体	aDesk-STD-100	40	2016	120.0
云服务器	RD650	2	2016	164.0

9. 申请增设专业的理由和基础

一、开设网络空间安全专业的理由

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变人们的生产生活方式，深刻影响人类社会历史发展进程。然而，网络空间安全形势日益严峻，国家政治、经济、文化、社会、国防安全及公民在网络空间的合法权益面临严峻风险与挑战。

2016年12月27日，经习近平总书记直接领导的中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》。这一战略的及时出台表明我国已高度认识到网络空间安全在保障国家安全中的重要战略地位。在《国家网络空间安全战略》中明确指出，要实施网络安全人才工程，加强网络安全学科专业建设。2019年6月，工信部正式发布《国家网络安全产业发展规划》，明确指出增强网络安全产业发展的高端引领作用，保障网络时代国家安全利益，维护网络空间安全已经成为维护国家安全新的战略制高点。

2018年9月4日，广西壮族自治区人民政府公布了《中共广西壮族自治区委员会 广西壮族自治区人民政府关于深入实施大数据战略加快数字广西建设的意见》以及数字经济三年发展行动计划、数字社会建设三年行动计划的主要内容，提出了包含提升数字基础设施与数字技术支撑能力、加强网络和数据安全等六大重点任务，其中要求建立健全数字安全保障体系，强化关键基础设施和信息系统安全防护，强化网络数据资源安全保护，加快云安全服务发展，确保数据运转安全顺畅高效。

2022年12月，中共南宁市委网信办关于请予提供数字中国建设发展相关情况材料的函中，要求南宁学院提供网络空间安全人才的培养，于支撑南宁市数字中国的战略部署。按照国家相关部署及结合经济社会发展，广西网络空间安全面临如下挑战和机遇。

第一，广西经济社会发展和创新驱动发展战略的要求。

随着经济与社会的发展，各领域信息化、网络化、智能化水平越来越高，各行业对于网络空间安全的重视程度会更加提高。《广西壮族自治区自然资源网络安全和信息化“十四五”规划（2021-2025年）》期间全面提升信息通信业网络安全监管、服务和保障能力水平，重点支撑“数字平安广西”建设。同时推进中国-东盟信息港建设，大力推进“数字广西”建设，做大做强广西数字经济，广西实施“创新驱动”发展战略，努力提升信息化水平，强化关键信息基础设施保护，提升网络空间安全保障能力，这是网络空间安全的挑战，也是推进“富民兴桂”事业的必然要求和重大发展机遇。

第二，广西网络空间安全面对新技术、新应用和新模式的需求。

社会发展日益向网络化、数据化趋势迈进，孕育了快速发展且空间广阔的网络空间安全市场，同时云计算、移动互联网、物联网、大数据、智慧城市等新技术、新应用和新模式的出现，亦将不断催生新的网络空间安全需求。广西已进入工业化、城镇化加速发展阶段，信息化是现代化的保障，强化创新驱动和推动信息技术的广泛深入应用，信息化建设不断加速，促使了网络空间安全技术与应用需求不断扩大，结合中国-东盟市场应用环境的网络空间安全行业市场需求持续增长，并催生全新的网络空间安全应用领域，从而为广西网络空间安全有效拓展市场提供机遇。

第三，尚未定型的竞争格局带来广西网络空间安全行业发展的空间。

我国网络空间安全行业正处于快速成长期，尚缺乏具有绝对垄断优势的大型网络空间安全企业。目前，网络空间安全市场需求呈多元化发展的趋势，行业内相关厂商通过差异化定位为用户提供各类网络空间安全产品。网络空间安全行业各细分领域的技术差异程度较高，市场竞争主要集中在各细分领域的专业厂商之间。广西和东盟国家经济发展水平接近，经济结构也有很多相同的地方，因此，广西将面临东盟国家信息化安全产业和市场的激烈竞争。未来，随着网络空间安全市场快速增长和竞争程度加剧，率先在技术研发方面掌握有核心竞争力，对广西乃至中国-东盟自由贸易区的企业将更多分享网络空间安全产业大发展带来的机遇。

第四，广西地缘优势形成网络空间安全发展的机遇。

全球经济结构面临新一轮调整，电子信息产品制造业的梯次转移，西部大开发战略的实施，“长三角”、“泛珠三角”区域合作的推进，中国-东盟自由贸易区的建立等，以上几大历史性机遇千载难逢。在新的形势下，机遇与挑战并存，广西地缘区位在中国经济发展中有着特殊的地位，面临着加快发展网络空间安全产业的极好机遇，只要努力把广西的地缘优势转化为经济优势，广西经济快速发展的黄金时代必然到来。充分发挥和利用广西地缘优势，可以提高广西网络空间安全技术的研究水平，加强信息化与网络空间安全基础设施建设，充分利用和合作开发他国各种优势资源，确保和稳固广西作为中国-东盟信息网络中心的地位和作用，增强广西的国际竞争力。

从以上分析可知，网络空间安全问题越来越复杂和重要，确保网络空间安全，更是中国-东盟自由贸易区实现科学发展、跨越发展中面临的一个必须高度重视的现实问题。无论是全国，还是基于中国-东盟自由贸易区的广西网络空间安全产业发展，必须通过完善

政策环境，加强网络空间安全技术产品的自主创新（研发）体系的建设，加强网络空间安全人才培养力度，才能走出一条广西网络空间安全产业的特色发展、科学发展之路。

二、南宁学院支撑该专业发展的学科基础

面对国内外网络空间安全人才需求、学科建设与行业兴起，南宁学院正积极投身其中，为国家和地区建设急需专业人才的培养贡献自己的力量，并推动教育观念、教学方法的革新。南宁学院坚持社会主义办学方向，坚持非营利性办学原则，坚持地方性、应用型办学定位，积极探索应用技术大学的办学道路，贯彻“应用型、开放式、新体验”的办学理念，以“质量发展、特色发展、创新发展”为主题，以人才培养为中心，以专业与课程建设为核心，以产教融合协同育人为重心，铸造应用型特色之魂、立稳服务地方发展之根、强固产教融合之本，努力为新时代区域经济社会发展培养高素质应用型人才。目前，学校已成为国家首批应用技术大学试点高校、广西新增立项建设硕士学位授予单位、广西新建本科学校转型发展试点学校、自治区首批深化创新创业教育改革示范高校、广西应用型本科高校联盟副理事长兼秘书长单位。

第一，计算机学科建设具有一定的规模和影响力，专业实训条件好。

信息工程学院是南宁学院办学历史最悠久的学院之一，前身为邕江大学计算机系。学院现有计算机科学与技术、通信工程、物联网工程 3 个本科专业，是南宁学院“电子信息”硕士点建设单位。申报的“网络空间安全”专业属于学校重点打造的六大专业集群的“信息与通讯技术”专业群。

学院目前获得自治区教学成果奖一等奖两项、二等奖两项、三等奖一项，1 个区级一流本科专业建设点、2 个区级民办重点本科专业，5 门区级一流课程、2 门区级课程思政示范课程，1 个区级虚拟教研室建设试点、1 个南宁学院首批虚拟教研室建设试点，1 个自治区级课程思政示范基层组织，2 个自治区级课程思政教学名师与团队。计算机科学与技术专业和物联网工程专业均以“四星”通过自治区的专业综合评估。

拥有教育部-ICT 产教融合创新基地 1 个，广西实验教学中心 1 个，广西自治区级校企协同育人平台 1 个，南宁市级公共实训基地 1 个，先进的实验设备和优良的教学条件，不但为学生提供了良好的学习环境，也使学院具备了较强的以新技术研发、新技术培训为主的社会服务能力。教育部-ICT 产教融合创新基地建设共投入 2500 余万元，占地 3000m²，主要包含物联网综合实验室、通信工程基础实验室、系统集成实验室、网络与安全实验室、数据科学实验室等 18 个专业实验室（平台）。

学院信息安全实训平台总投资 200 万，是一个为计算机科学与技术、物联网工程、数据科学与大数据技术等本科专业专门用于开设网络实训课程的专业实验室。通过实验，可以使学生加深对网络功能配置、网络安全概念、黑客攻防原理和常用安全加密手段的理解，让学生对网络设计、网络安全、信息安全有一个整体的理解和掌握，拓宽学生知识面，提高动手实践能力。

第二，校企深度合作，打造应用型混编师资，建设有成效。

学院专任教师队伍中，副高级以上职称 24 人（占 68.57%），博士、硕士学位 31 人（占 88.57%），博士生导师 3 人、硕士生导师 5 人。由高校教师和来自行业知名企业的工程师组成的“混编型”专业教学团队，为学院新一代信息技术的引进、课程开发、工程实践教育，以及应用型人才培养质量提升提供了有力保障。

学院紧跟学校应用技术大学建设发展思路，认真践行学校“应用型、开放式、新体验”的办学理念，坚持校企合作专业发展路径、培育“产教融合、协同创新”的人才培养模式特色。学院从 2012 年起，先后与中兴通讯、北京华晟、华为等知名企业建立建立校企混编师资队伍，获自治区级首批虚拟教研室团队 1 个、自治区级课程思政示范基层教学组织 1 个、自治区级课程思政教学名师与团队 2 个。校企混编师资队伍的建设，有效保障了学生的培养质量。

三、南宁学院网络空间安全专业发展规划

南宁学院目前已开办了计算机科学与技术、物联网工程、数据科学与大数据技术等与网络空间安全相关本科专业，开设网络空间安全本科专业对上述专业将产生深远影响，总体上有利于学校办学格局的调整和优化。规划思路如下：

第一，市场为需求为导向，制定网络空间专业体系规范，推动专业发展的多样化路径。

建立网络空间安全专业的体系规范、指导方针、评估和激励机制。改变应用型本科专业和行业需求之间的割裂状态，将职业知识技能要求融入教学计划，促进专业建设与地方经济需求无缝对接。通过开展紧密的校企合作，利用华为合作企业的优势，打造校企混编师资队伍，建立专业实践体系建设，撰写专业应用型教材编写。将网络空间安全基本知识能力体系融入信息技术类专业，作为核心知识模块，扩大网络空间安全人才培养的基础。促进网络空间安全专业的多样化发展。

第二，发挥深度合作企业“华为”优势，建立网络空间安全专业知识和技能素质培养框架，优化人才培养体系。

发挥校企深度合作企业“华为”公司的优势，优化学校与企业的网络空间安全人力资源，针对岗位、知识、技能和素质的具体需求，持续改进培养机制和更新课程体系，培养广西社会经济急需的人才。与华为公司建立职位培养认证机制，对网络空间安全专业培养方案和课程体系进行认证。完善人才培养体系，以创新能力培养为核心目标，建立专业与创新的“双主线”培养模式，实施相应的选拔、评价、激励和退出机制。强化创新能力和工程实践能力的培养。

第三，借助学校重点打造“信息与通讯技术”集群，发挥产教融合的作用，建设网络空间安全专业。

借助学校重点打造“信息与通讯技术”集群，及建设“电子信息”硕士点的优势，打造网络空间安全专业，将网络安全理念和实践融入信息技术类专业、安全融入专业技能中。通过跨学院、跨专业的多种交叉培养方式，构建网络安全课程体系和实验实训体系。培养符合网络与信息安全产业需求的高级工程技术人才，具备解决复杂网络与信息安全工程问题的能力、综合工程技能、系统的科研和学习能力，以及复杂社会问题的处理能力，并具有责任感和组织与领导力。建立高校与行业主管部门、网络空间安全相关企事业单位、科研院所、社会用人单位的深度合作机制，鼓励合作制定人才培养目标、共同开设相关课程和编写教材，实现网络空间安全人才培养与广西地方网络安全发展需求的紧密结合。

10. 校内专业设置评议专家组意见表

总体判断拟开设专业是否可行		☒ 是 ☐ 否
理由： 网络空间安全专业作为一个新兴专业，人才供不应求。中共南宁市委网信办等政府部门和相关企业要求南宁学院提供网络空间安全人才的培养，支撑南宁市数字中国的战略部署，加强网络空间安全人才培养力度，才能走出一条广西网络空间安全产业的特色发展、科学发展之路。信息工程学院是南宁学院“电子信息”硕士点建设单位。申报的“网络空间安全”专业属于学校重点打造的六大专业集群的“信息与通讯技术”专业群，学院拥有一批结构比较合理老中青相结合的师资队伍，教育教学成效显著，获得区级教学成果奖一等奖两项、二等奖两项，建设一批区级一流本科专业和课程，学院还与华为等知名企业建立校企混编师资队伍，良好师资队伍有效保障学生的培养质量。学院拥有教育部-ICT 产教融合创新基地、广西自治区级校企协同育人平台和南宁市级公共实训基地，可提供良好专业的实验设备和优良的教学条件。南宁学院目前已开办了计算机科学与技术、物联网工程、数据科学与大数据技术等与网络空间安全相关本科专业，开设网络空间安全本科专业有利于学校办学格局的调整和优化，申报专业人才培养方案科学合理，有较好的适应性。 综上，南宁学院拟开设的网络空间安全专业优势明显，具备开设条件，专家组一致同意开设。		
拟招生人数与人才需求预测是否匹配		☒ 是 ☐ 否
本专业开设的基本条件是否符合教学质量国家标准	教师队伍	☒ 是 ☐ 否
	实践条件	☒ 是 ☐ 否
	经费保障	☒ 是 ☐ 否
专家签字： 		